



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.  | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------|------------------|
| 10/517,780   | 12/28/2004  | Tomoyuki Asano       | 262954US6PCT        | 7690             |
| 22850  | 7590        | 12/28/2009           |                     |                  |
| OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.<br>1940 DUKE STREET<br>ALEXANDRIA, VA 22314 |             |                      |                     |                  |
| EXAMINER   |             |                      |                     |                  |
| NILFOROUSH, MOHAMMAD A   |             |                      |                     |                  |
| ART UNIT   |             | PAPER NUMBER         |                     |                  |
| 3685   |             |                      |                     |                  |
| NOTIFICATION DATE  |             | DELIVERY MODE        |                     |                  |
| 12/28/2009   |             | ELECTRONIC           |                     |                  |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com  
oblonpat@oblon.com  
jgardner@oblon.com

### Office Action Summary

**Application No.**

10/517,780

**Applicant(s)**

ASANO, TOMOYUKI

**Examiner**

Mohammad A. Nilfroush

**Art Unit**

3685

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 05 October 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 5-33 and 37-42 is/are pending in the application.
- 4a) Of the above claim(s) 5-33 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 37-42 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/GS/US)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Acknowledgements***

1. The amendment filed 5 October 2009 is acknowledged.
2. Claims 5-33 and 37-42 are pending.
3. Claims 37-42 have been examined.
4. This Office action is given Paper No. 20091214 for reference purposes only.

***Continued Examination Under 37 CFR 1.114***

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5 October 2009 has been entered.

***Response to Amendment/Arguments***

6. The amendment of claim 37 overcomes the rejection of claims 37-38 under 35 USC §101.
7. Applicant's arguments with respect to claims 37-42 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 37-42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 37, 39, and 41 recite "...generating...a plurality of different signature data elements from a secret key data element and a message data element; generating...a plurality of different identification data elements, each of the plurality of different identification data elements including a generated signature element and the message data element used in the generating of the generated signature data elements..." However, the specification does not describe a plurality of different signatures being created using only a single secret key and message.

Claims 38, 40, and 42 are also rejected as each depends on claims 37, 39, and 41 respectively.

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 37-42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
12. Claims 37, 39, and 41 recite "...generating...a plurality of different signature data elements from a secret key and a message data element..." A digital signature is a function of the data being signed and the key used to sign it (An Introduction to Cryptography, Page 19, Figure 1-6). Thus, it is unclear to one of ordinary skill one of ordinary skill how multiple different signatures can be produced when both the data being signed, and a key used to generate the signature, are the same.

Claims 38, 40, and 42 are also rejected as each depends on claims 37, 39, and 41 respectively.

***Claim Rejections - 35 USC § 103***

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 37-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano, et al. (European Patent Application Publication No. EP 1069567, hereinafter "Asano") in view of Muehring (US Patent Application Publication No. 2003/0145183) in further view of Ohta, et al. (US Patent No. 6,212,637, hereinafter "Ohta").

15. Regarding claims 37, 39 and 41, Asano discloses a method of a media verification system for identifying recording media, comprising:

- generating a plurality of different signature data from secret key data and message data using a data processing device of the media verification system (Asano Paragraphs **37**, and **115**);
- generating a plurality of different identification data using the data processing device, each of the plurality of different identification data including a generated signature data and a message data used in the generating of the generated signature data (Asano Paragraphs **37**, and **115**);
- assigning one of the plurality of generated identification data to each of a plurality of different recording media (Asano Paragraphs **27-28**, **37**, **43**, and **115**);
- recording one of the plurality of generated identification data to an assigned recording media using a media writing device of the media verification system (Asano Paragraph **28**, **39**, **43**, and **115**);
- generating verification data from the generated signature data of the identification data recorded on the assigned recording media using a public key (Asano Paragraphs **35**, **46**, **51-60** and **115**);
- comparing the verification data to the message data of the identification data recorded on the assigned recording media using the data processing device and verifying the identification data if the verification data is the same as the message data of the identification data recorded on the assigned recording media (Asano Paragraphs **55-60**);

- writing an encrypted content to the assigned recording media using a media recording device if the assigned recording media is verified in the comparing, wherein the media recording device is configured to inhibit writing the encrypted content to a recording media having an unverified identification data or no identification data recorded thereon (Asano Paragraphs **61, 72, 81-82, 90-92, and 115**; Claim **1**).

Asano does not specifically disclose storing the plurality of different identification data in an electronic memory of the media verification system. Asano further does not specifically disclose that the plurality of different signature elements are produced using the same message data.

Muehring discloses storing the unique identification information stored on each disc on a server (Muehring Paragraph **18**).

Ohta discloses generating a signature using based on data that includes elements that are constant (Ohta **12:23-25; 13:4-28**, public information {p, q, g}).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Asano to include storing the unique identification information stored on each disc on a server as disclosed in Muehring in order to track where the disc is recorded and make sure data is only recorded on valid discs (Muehring Paragraphs **18-20**). Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Asano in view of Muehring to include using constant data elements in generating signatures as disclosed

in Ohta in order to decrease computational load on a signer apparatus by using the Schnorr scheme of generating a digital signature (Ohta **2:41-60**; **11:54-57**).

16. Regarding claims 38, 40, and 42, Asano discloses:

- generating an identification revocation list, wherein the identification revocation list includes identification data (Asano Paragraphs **41-42**);
- recording the identification revocation list to the assigned recording media using the media writing device, wherein the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media if the identification data recorded on the assigned recording media is included in the identification revocation list (Asano Paragraphs **43, 53-55**).

Asano does not specifically disclose that the identification data on the revocation list corresponds to an unauthorized recording media.

Muehring further discloses storing disc IDs on a server and marking pirated copies as such (Muehring Paragraphs **18** and **33**).

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Rankl, W. and W. Effing, "Smart Card Handbook," Second Edition, 2000, John Wiley & Sons, Ltd., West Sussex, England., for disclosing the use of constant values in calculating a signature.



Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad A. Nilforoush whose telephone number is (571)270-5298. The examiner can normally be reached on Monday-Thursday 10 am - 6 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on (571)272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. A. N./  
Examiner, Art Unit 3685

/Calvin L Hewitt II/  
Supervisory Patent Examiner, Art Unit 3685